

Technology-assisted epidemiological contact tracing solutions apparently clash with civil liberties: a survey, and a proposal

Giacomo Fabris, Andrea Nicoletto

March 18, 2020

1 Background

If you opened a newspaper in the last month you may want to skip this chapter.

It is well known that in late 2019 a new virus, SARS-CoV-2, emerged in the city of Wuhan, China[1]. The virus infects humans causing a respiratory infection which may cause severe symptoms in a minor share of the infected population. The contagion rapidly spread to (most of) the entire world[2] and is causing major strain on national health systems.

During the month of January 2020 China enacted measures aimed at containing the virus, which had spread wildly in the Hubei region[3]. Such measures included a forced quarantine of multiple weeks for the entire population of various Chinese regions, general travel restrictions and the extensive tracing of the population movements through technological means. The Chinese way to deal with the virus is deemed to be effective in stemming the contagion, while questions are raised on the compatibility of such measures with liberal democracies, i.e. whether it is actually possible, both legally and practically, to enact them in Western countries.

Italy has been severely affected with the contagion of SARS-CoV-2 starting from the month of February 2020. As of March it became clear that community spreading was occurring in most European nations, which have imposed some kind of containment strategy, e.g. ban on social gatherings, closing of shops of nonessential goods, travel restrictions. The most draconian measures are enacted in Italy, which also imposed a mandatory stay-at-home obligation for the entire population, with the exception of states of necessity and commuting for those unable to work remotely.

It shall be noted that some Far East countries neighboring with China (e.g. Singapore, Taiwan, Japan) have been to date effective in containing the contagion, with little or no community spreading; South Korea experienced a spike in cases which have been efficiently curbed in a matter of weeks. To date, none of these countries has introduced nation-wide lockdowns.

There are ongoing efforts in order to produce a vaccine against the virus[4], which is expected to be available no earlier than the beginning of 2021.

2 Introduction

At the time of writing, heavy lockdown measures are enacted in Italy in order to try to contain the spread of the SARS-CoV-2 virus. The lockdown started on March, 10 and will last until April, 3[5, 6]; even though these measures might be further extended.

The consensus is that the lockdown will stem the contagion in a matter of weeks; controlling the number of new cases is essential in order to allow the national health service to effectively treat the patients with severe symptoms.

However, little is known about which are the expectations of European governments about the situation in the following months. While there is some hope that the hot season will help reducing the contagion[7], it shall be noted that outbreaks are currently ramping up in countries with a hot climate, such as Malaysia.

Since it is unlikely that the lockdown measures will completely eradicate the virus, it is evident that a clear and effective strategy shall be designed to cope with new contagions in the following months, which shall be quickly contained in order to avoid vaster outbreaks which could require a new enacting of lockdown measures.

3 Debate on containment measures

Italian policymakers, officials and journalists are debating about which measures are the most effective in controlling the contagion after the current emergency phase will terminate. There is a consensus in following the “South Korean model”, i.e., according to the proponents, tracking the movements of the persons in order to be able to efficiently perform contact tracing of newly confirmed cases. Many propose to acquire data from mobile network carriers in order to track each person’s mobile phone both for contact tracing and to enforce quarantine orders of infected or suspected cases.

It shall be noted that, while South Korea seems to be containing the outbreak efficiently, its technology-assisted contact tracing solution is only one of several measures which are enacted, part of a comprehensive plan which have been designed way before the surge of cases[8]. Moreover, it is not known whether the South Korean experience could be generalized to Western countries. Actually, South Korea’s ways of doing contact tracing do not include a continuous monitoring of the mobile phone’s position; rather, they search *ex post* electronic footprints such as electronic payments, CCTV, hotels registrations and similar[9]. Such information is made public on the government website and, even if it is made anonymous, a precise breakdown of the movements of a person’s daily routine makes it easy to associate these logs to the person’s name. In case you are wondering how data can be de-anonymized, you might want to read the excellent reportages of NYT’s Privacy Project, as an introduction.[10]

The legitimacy of such measures with respect to human rights is dubious at best, as it is clear that movements may reveal personal information, including but not limited to, previous health issues, sexual orientation, religious beliefs, political orientation. Harassment and social stigma are among a wide range of consequences which may occur for an indefinite period of time after these data are leaked, a period which will be way longer than the actual course of the outbreak.[11]

Invasive contact tracing methods are starting to be used also in Israel, where opposition parties and privacy activists are raising concerns that this may lead to mass surveillance and harm civil rights. [12]

It has been reported that China is actively tracking its citizens[13, 14], and is able to use this information to perform contact tracing and evaluate the opportunity to tight or loose the lockdown in a given region, even on a per-person basis. Of course, this system is part of China’s intensive mass surveillance program, which is also used for law enforcement[15], social control and dissent eradication. It should be unnecessary to list the reasons why enforcing such measures in Western countries would not be desirable[16].

Some may think that, during an epidemic, the State shall be allowed to enforce

emergency measures and therefore such measures may be applied, for a limited period of time. Maybe they are even aware of the human rights concerns that I outlined before, but they hold it to be a necessary evil. I think that those who actually believe this either have a vague understanding of the issue or have some degree of fetishism to autocracies. Anyway, let me state the following very obvious considerations.

1. Such systems are complex, and when built, are there to stay. They will track every citizen continuously, and you may only hope that they are turned off during non-emergency periods. Many people will have access to those systems, and use it in non-compliant ways, both in the private companies operating the networks and in the government agency delegated to use these data when deemed necessary. The economical value of these data is enormous, and will give an incredible advantage to every player which will be able to have access to it[17]. Moreover, they are a giant honeypot for every foreign or subversive power, which can hack the system and use it for malicious purposes.
2. A strict definition of “emergency” is necessary, and strong checks and balances are required, if we do not want to give a future government the capability to track citizens massively and indiscriminately. Note that the severe lockdown measures enacted in Italy, which heavily limit civil liberties, came into power with a mere administrative act of the government, without any parliamentary approval or control[5, 6]. Such measures include fines and jail periods for those who do not comply to the act, and to date charges have been already filed against more than 40,000 citizens[18], which is comparable to the number of confirmed cases of SARS-CoV-2 infection in Italy[19]. Time will tell whether that act was legitimate or not with respect to the powers given to the government by the Italian constitution; anyway, it is not unforeseeable that with similar acts an emergency situation may be declared e.g. for law enforcement issues in order to be able to access these tools.

It shall also be noted that merely accessing to the data provided by the mobile carrier is useless for contact tracing, as the error is, in the best case, around 100m (when multiple base stations are in reach of a deployed LTE network with OTDOA capabilities)[20]. Positioning in rural contexts, with a lower number of base stations within reach and/or older network technologies is completely unreliable. While useless for contact tracing, the only application I may foresee for such a system in an epidemic scenario is the enforcement of quarantine/stay-at-home orders, which could be anyway easily circumvented by leaving the phone at home. The argument that private companies (e.g. Google) are already tracking us in order to provide us their location services, and therefore sharing data also with the government is a non-issue, is clearly invalid. These services are opt-in, private companies do not exert on us any authoritative power and are subject to the vast range obligations mandated by EU Regulations (GDPR). In contrast, state authorities have no obligation to comply with the GDPR for such activities (Art. 2 EU Reg. 2016/679)[21].

4 If we really want to go that way: requirements of a non-orwellian contact tracing app

It may well be argued that the help of location technologies is fundamental in establishing a successful contact tracing technology. However, we shall define strict and precise requirements for such technology so that it could coexist with a liberal democracy.

First and foremost, it is fundamental to build a distributed systems, in which there is no data bank retained by some governative agency and a continuous stream of surveillance data in transit in the network. Rather, contact tracing data shall remain in control of the user, and be communicated to others only if necessary (i.e., if the user has tested positive to the virus). Therefore, rather than building a surveillance infrastructure, the proposal consists in equipping every user with an application on their smartphone, which participates to the contact tracing network. The application shall be distributed as Free Open Source Software, so that its functionalities may be transparently assessed by everyone. I think that collecting location data is not feasible nor necessary. Indeed, it is not even desirable, given the privacy concern which follow the publication of the list of positions the infected user has been to. Precision is too low, even for GPS: the actual precision of a smartphone antenna is unlikely to be better than 5 meters, namely, the opposite sidewalk of the street[22]. Moreover, GPS is useless for indoor positioning, which is where contacts are likely to occur.

Therefore, I suggest to evaluate the feasibility of a Bluetooth/BLE-enabled tracking technology. Every device could emit a short ping containing a UUID which is refreshed frequently (e.g. 5 minutes); the refresh time is coordinated among the network (time alignment precision issues are not relevant, precision offered by the NTP protocol is more than enough for this scenario). The transmission frequency of pings could vary between 10 seconds and 1 minute, depending on the accelerometer data of the device (i.e. shorter period while walking, longer period while standing still/sitting). Devices in range shall keep track of the advertised UUID if the received strength is higher than a threshold (meaning that the two devices were near) and the timestamp of the encounter. Of course, the application may be switched off when it is not necessary to emit any ping (i.e. while the user is at home).

In case the user is found to be positive to the virus, they will distribute to all other users over the Internet the list of pings they transmitted during their travels in the last few days. Sharing of such information could be done using peer-to-peer network topologies, which could be segregated per province or region in order to avoid an excessive amount of non relevant data to be shared. Rather than directly sharing the list of UUIDs, the contagious user will compute the hash of the combination of the UUID and its validity period. In this way it becomes less feasible to perform temporal graph analysis on the encounter patterns.

This application would have the following advantages with respect to the proposals currently circulating.

1. The system is transparent, its behaviour can be assessed independently and there are no single point of failures.
2. Users willingly and consciously participate in the data collection project.
3. No position data is collected. Users which never become contagious are never required to share their data, while the data shared by contagious users is effectively anonymized and does not contain any position information.
4. The collected data is meaningful, because it actually corresponds to a close contact and works in every scenario (both indoor and outdoor, accounting of physical barriers which would block both the RF signal and the virus spread).
5. The cost of such system is minimal.

Of course, as nothing is perfect, there are disadvantages as well:

1. The increased RF usage will have an impact on smartphones' battery drain, which is anyway less than the drain the user experiences while using e.g. Bluetooth earphones.
2. It is necessary to have a proactive adoption from users in order to make the system work.

As soon as a protocol standard is published, custom hardware could also be built to address battery drain problems and to equip users which do not have any smartphone (e.g. kids). Small Bluetooth trackers, which could be carried in a pocket and have a battery life of days, could be manufactured with a production cost which I estimate could be less than 20 USD. The communication with the rest of the distributed network is done linking the tracker with a smartphone or a PC, e.g. at the end of the day.

5 Conclusion

The pandemic caused by the SARS-CoV-2 virus has dramatically changed the daily life of billions of people in the world and caused vast economic damage. Time will pass before the virus will not represent a menace to people and medical facilities: technology could surely be a valid instrument with which our society could ease lockdown measures and facilitate the containment efforts. However, there are clear dangers in establishing a massive surveillance program, which could not be simply ignored because of the emergency situation. The contagion surely has a toll on human life, but so have surveillance programs too.

I do think that the unpreparedness w.r.t. a pandemic which spreads in a similar way of the periodic (though not frequent, luckily) influenza pandemics is a clear strategic failure of Western countries. I do think either that it is not sound to hurry technology-assisted tracking projects during an emergency situation, given their vast implication in our daily life. We shall not be driven by fear or urgency, rather, a rational and democratic debate shall be carried out, when things will settle down, about how we shall prepare for the next pandemic.

References

- [1] Na Zhu et al.
“A Novel Coronavirus from Patients with Pneumonia in China, 2019”.
In: *New England Journal of Medicine* 382.8 (2020), pp. 727–733.
DOI: 10.1056/NEJMoa2001017.
- [2] The New York Times. *Coronavirus Map: Tracking the Global Outbreak*. Feb. 2020.
URL:
<https://www.nytimes.com/interactive/2020/world/coronavirus-maps.html>
(visited on 03/19/2020).
- [3] David Cyranoski. *What China's coronavirus response can teach the rest of the world*. Mar. 2020.
URL: <https://www.nature.com/articles/d41586-020-00741-x> (visited on 03/19/2020).

- [4] Syed Faraz Ahmed, Ahmed A. Quadeer, and Matthew R. McKay. “Preliminary Identification of Potential Vaccine Targets for the COVID-19 Coronavirus (SARS-CoV-2) Based on SARS-CoV Immunological Studies”. In: *Viruses* 12.3 (2020). ISSN: 1999-4915. DOI: 10.3390/v12030254. URL: <https://www.mdpi.com/1999-4915/12/3/254>.
- [5] Giuseppe Conte. “Decreto del Presidente del Consiglio dei Ministri 8 marzo 2020”. In: *Gazzetta Ufficiale della Repubblica Italiana* 59 (Mar. 2020). URL: https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2020-03-08&atto.codiceRedazionale=20A01522&elenco30giorni=false (visited on 03/19/2020).
- [6] Giuseppe Conte. “Decreto del Presidente del Consiglio dei Ministri 9 marzo 2020”. In: *Gazzetta Ufficiale della Repubblica Italiana* 62 (Mar. 2020). URL: https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2020-03-09&atto.codiceRedazionale=20A01558&elenco30giorni=false (visited on 03/19/2020).
- [7] Lia van der Hoek. “Human coronaviruses: what do they cause?”. In: *Antiviral Therapy* 12 (2007), pp. 651–658.
- [8] Dennis Normile. *Coronavirus cases have dropped sharply in South Korea. What’s the secret to its success?* Mar. 2020. URL: <https://www.sciencemag.org/news/2020/03/coronavirus-cases-have-dropped-sharply-south-korea-whats-secret-its-success> (visited on 03/19/2020).
- [9] Korea Centers for Disease Control & Prevention COVID-19 National Emergency Response Center Epidemiology & Case Management Team. “Contact Transmission of COVID-19 in South Korea: Novel Investigation Techniques for Tracing Contacts”. In: *Osong Public Health Res Perspect* 11.1 (2020), pp. 60–63. DOI: 10.24171/j.phrp.2020.11.1.09. URL: <http://ophrp.org/journal/view.php?number=538>.
- [10] Stuart A. Thompson and Charlie Warzel. *How to Track President Trump*. Dec. 2019. URL: <https://www.nytimes.com/interactive/2019/12/20/opinion/location-data-national-security.html> (visited on 03/19/2020).
- [11] Mark Zastrow. *South Korea is reporting intimate details of COVID-19 cases: has it helped?* Mar. 2020. URL: <https://www.nature.com/articles/d41586-020-00740-y> (visited on 03/19/2020).
- [12] Judah Ari Gross. *Netanyahu sparks privacy scare with move to track corona patients’ phones*. Mar. 2020. URL: <https://www.timesofisrael.com/netanyahu-sparks-privacy-concerns-with-move-to-track-corona-patients-phones/> (visited on 03/19/2020).
- [13] Paul Mozur. *Inside China’s Dystopian Dreams: A.I., Shame and Lots of Cameras*. July 2018. URL: <https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html> (visited on 03/19/2020).

- [14] Charlie Campbell.
How China Is Using “Social Credit Scores” to Reward and Punish Its Citizens.
Jan. 2019. URL: <https://time.com/collection/davos-2019/5502592/china-social-credit-score/> (visited on 03/19/2020).
- [15] Paul Mozur and Aaron Krolik.
A Surveillance Net Blankets China’s Cities, Giving Police Vast Powers. Dec. 2019.
URL:
<https://www.nytimes.com/2019/12/17/technology/china-surveillance.html>
(visited on 03/19/2020).
- [16] Matthew Guariglia and Adam Schwartz.
Protecting Civil Liberties During a Public Health Crisis. Mar. 2020.
URL: <https://www.eff.org/deeplinks/2020/03/protecting-civil-liberties-during-public-health-crisis> (visited on 03/19/2020).
- [17] Stuart A. Thompson and Charlie Warzel.
Twelve Million Phones, One Dataset, Zero Privacy. Dec. 2019.
URL: <https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html> (visited on 03/19/2020).
- [18] Lorenzo Tondo. *Italy charges more than 40,000 people with violating lockdown.*
Mar. 2020. URL: <https://www.theguardian.com/world/2020/mar/18/italy-charges-more-than-40000-people-violating-lockdown-coronavirus> (visited on 03/19/2020).
- [19] Ministero della Salute. *Covid-19: i casi in Italia alle ore 18 del 19 marzo.*
Mar. 2020. URL: <http://www.salute.gov.it/portale/nuovocoronavirus/dettaglioNotizieNuovoCoronavirus.jsp?lingua=italiano&menu=notizie&p=dalministero&id=4272> (visited on 03/19/2020).
- [20] Ericsson. *Positioning with LTE.* Sept. 2011.
URL: <https://www.sharetechnote.com/Docs/WP-LTE-positioning.pdf> (visited on 03/19/2020).
- [21] *Regulation (EU) 2016/679 of the European Parliament and of the Council.*
Apr. 2016.
URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e2172-1-1> (visited on 03/19/2020).
- [22] Yuki Odaka et al. “Error Analysis of the Mobile Phone GPS and Its Application to the Error Reduction”. In: SENSIG ’10/MATERIALS’10 (2010), pp. 35–40.
DOI: 10.5555/1950175.1950184.